SELFNET Framework self-healing capabilities for 5G mobile networks

Santos, José Pedro ; Alheiro, Rui ; Andrade, Luís ; Caraguay, Ángel Leonardo Valdivieso ; López, Lorena Isabel Barona ; Monge, Marco Antonio Sotelo ; Villalba, Luis Javier García ; Jiang, Wei ; Schotten, Hans ; Alcaraz Calero, Jose M.; Wang, Qi; Barros, Maria João

Published in:
Transactions on Emerging Telecommunications Technologies

DOI:
10.1002/ett.3049

E-pub ahead of print: 21/06/2016

Document Version
Peer reviewed version

SELFNET Framework self-healing capabilities for 5G mobile networks

José Pedro Santos, Rui Alheiro, Luís Andrade, Ángel Leonardo Valdivieso Caraguay, Lorena Isabel Barona López, Marco Antonio Sotelo Monge, Luís Javier Garcia Villalba, Wei Jiang, Hans Schotten, Jose M. Alcaraz-Calero, Qi Wang, Maria João Barros

Abstract

Nowadays, mobile networks are complex sets of heterogeneous equipment that use proprietary management applications, resulting in a huge expenditure, a large effort and a time-consuming process to manage all network elements by means of currently manual or semi-automatic approaches. With the emergency of new technologies, such software-defined networking, network function virtualization, and cloud computing, the current configurable networks are capable of becoming programmable, which will facilitate advanced autonomous network management. This article presents capabilities of a novel framework proposed by the SELFNET project that enables highly autonomic management functionalities. It focuses on the proposed self-healing use case that can be applied to reactively or preventively deal with the detected or predicted network failures. The SELFNET can provide the upcoming 5G system: an autonomic management framework, which brings a remarkable reduction upon operational expenditure and a substantial improvement of quality-of-experience (QoE) in terms of reliability, availability, service continuity and security.

1 Introduction

As of today, network operators have to deal with network problems, for example, link failures, security attacks, quality-of-service (QoS) degradation, software bugs and hardware faults, manually or semi-automatically. Troubleshooting these issues typically require manual re-configuration of equipment, and in some cases, the installation of new equipment and functionalities such as routers, network address translators, firewalls and load balancers, which cannot be performed without interrupting the normal operation of the network. It causes disruptions in the services and violations in service level agreements, as well as incurring increased operational and capital costs and compromised end users' quality-of-experience (QoE) [1]. That is why the operational expenditure (OPEX) of mobile operators is currently three times that of capital expenditure [2]. With the advance of new technologies, such as software-defined networking (SDN) [3, 4], Network function virtualization (NFV) [5-8] and cloud computing, the current configurable networks are capable of becoming programmable, which will facilitate advanced autonomous network management. The virtualized and software-defined network open the possibility of a scalable, programmable, extensible 5G networks with an autonomic network management functionalities, leading to a remarkable reduction upon OPEX and a substantial improvement of QoE in terms of reliability, availability, service continuity and security.

This problem motivates the setup of H2020 project Self-organized Network Management in Virtualized and Software-Defined Network (SELFNET) to design and implement an autonomic network management framework for providing self-organizing and intelligent network features in upcoming 5G mobile systems. SELFNET is capable of automatically detecting and mitigating a range of common network problems that are currently manually or semi-automatically addressed by network administrators. Three use cases captured most of the network management problem in current networks, that is, self-protection, self-optimization and self-healing, have been defined in SELFNET. Because of the space limitation, this paper only focuses on one of the main objectives of SELFNET, which is to provide self-healing functionalities in order to detect and avoid network failures of the network infrastructure. To be specific, the self-healing functionality of SELFNET covers the following scenarios:

- Proactive self-healing for resource and power supply. This scenario addresses the need of constant monitoring of the resources and power supply on the network infrastructures.
- Reactive self-healing in critical, disaster or unpredictable scenarios. This scenario addresses the need for a reactive self-healing functionality as a necessary backup.
- Proactive self-healing based on Network Slicing and Cyber-Footing Human Dynamics. This scenario addresses the need of new user groups with independent business models that depend on the availability of networking services. SELFNET based on collected historical references predicts high-resource demands before they happen and take actions about them.

This paper presents a brief overview of the proposed SELFNET architecture and the innovative self-healing capabilities that can be applied to deal with detected or predicted network failures in a reactive or preventive manner. The rest of this paper is organized as follows: Section 2 summarizes the SELFNET architecture. Section 3 describes a general overview of SELFNET self-healing capabilities. For its part, Section 4 introduces the proactive self-healing concept for resource supply and Section 5 promotes the case of reactive self-healing in critical and unpredictable scenarios. Section 6 introduces the possibility of proactive self-healing based on Network Slicing and Cyber Footing Human Dynamics. Section 7 exposes the contributions of the new self-healing management capabilities. Finally, Section 8 concludes this paper.

2 SELFNET General Overview

SELFNET provides a scalable, extensible and intelligent network management system by exploring the integration of new technologies (SDN [9], NFV [10], cloud computing [11], artificial intelligence, among others). Therefore, SELFNET aims to help network operators to perform management tasks, such as the automatic deployment of SDN/NFV applications that provide automatic network monitoring and maintenance delivered by defining high-level tactical measures and enabling autonomic corrective and preventive actions to mitigate existing or potential network failures. SELFNET will address three major network management concerns by

providing self-protection capabilities against distributed network attacks, self-healing functionalities against detected or predicted network failures and malfunctions, and self-optimization features to dynamically improve the performance of the network and the QoE of the users. As depicted in Figure 1, the architecture is logically divided on five differentiated layers: infrastructure layer, virtualized network layer, SON control layer, SON autonomic layer, SON interface layer and NFV orchestration and management.

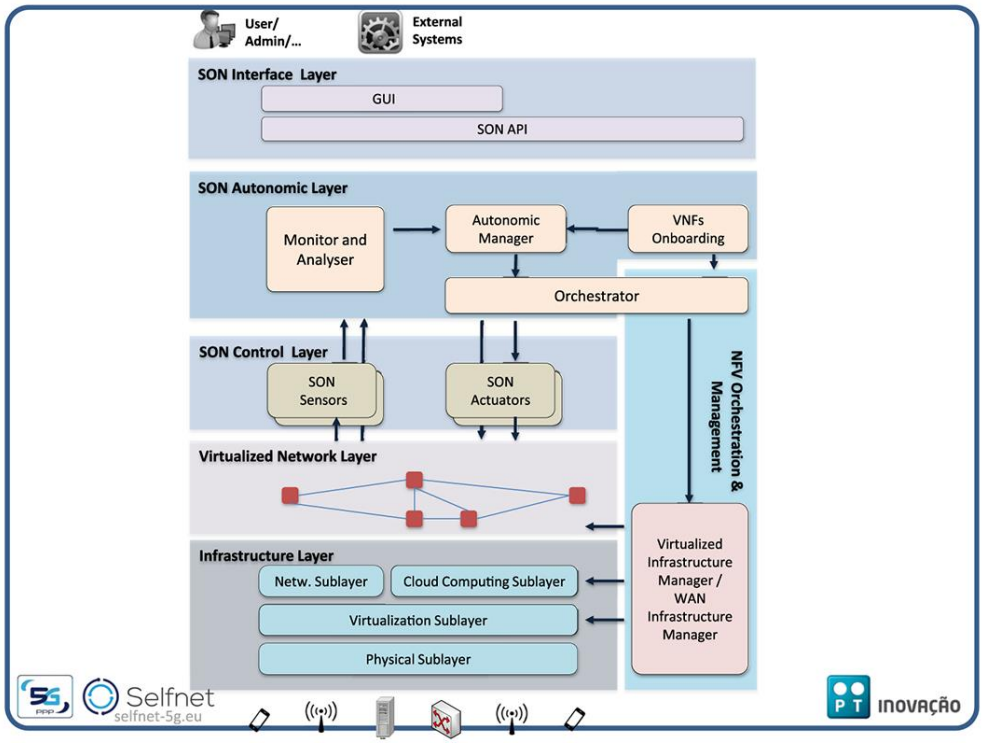

Figure 1. SELFNET architecture.

The infrastructure layer enables the instantiation of virtual functions (Computing, Networking and Storage) on the physical infrastructure. For this, the physical sublayer provides the physical connectivity and the virtualization sublayer enables the virtualization of the resources. The network and cloud computing sublayer adds multi-tenancy capabilities and provides functionalities to create, delete and manage virtual infrastructures. For its part, the virtualized network layer represents the deployed logical topology of the different network functions and virtual machines allocated in the virtual infrastructure. The SON control layer contains the SON sensors and SON actuators. On one hand, SON sensors collect information about the services running on network infrastructure. On the other hand, SON actuators will enforce actions into the network.

The SON Autonomic Layer provides the network intelligence. First, the monitor and analyzer module collects and stores all the data coming from sensors using a data management system. Then, advanced algorithms (data mining, pattern recognition, prediction algorithms) allow a comprehensive analysis of the received information. At this point, recognition of anomalous or suspicious behaviours based on health of network (HoN) metrics are performed. Meanwhile, the autonomic manager acts as the brain of the framework dealing with existing and/or potential network problems in both reactive and proactive ways. The artificial intelligence algorithms determine

resolution actions to be taken in the network. The actions can involve the use of services allocated on NFVs onboarding. The corresponding actions are coordinated by the NFV orchestration and management layer and the corresponding virtualized and infrastructure manager module. This layer enables the orchestrator with capabilities that allow the management and configuration of SDN/NFV Apps. It resolves the dependency, the execution order and priority of different actions and ensures that the SDN/NFV Apps are allocated with sufficient resources to perform their tasks.

This article focuses on the SELFNET self-healing capabilities that are expected to yield sustained quality of services under critical situations in terms of service continuity, availability and resilience by predicting or identifying network failures. In the next section, SELFNET self-healing use case is further addressed.

3 Self-healing Overview

The SELFNET self-healing use case aims to demonstrate how the self-healing capabilities of the SELFNET network management framework can be applied to deal with a wide range of detected or predicted network malfunctions and failures, leading to a remarkable reduction upon OPEX and an improvement of QoE/QoS provision in 5G systems. The self-healing SDN/NFV sensors will enable the detection of common failure/malfunction in the current network infrastructure, such as hardware/software failures/faults, infrastructure/operation vulnerabilities and power supply interruption issues. Then, SELFNET analyzes the information provided by the sensors and apply actions in order to mitigate the anomalies and recover the network infrastructure to a normal operating state. These recovery actions will be enforced by the use of self-healing actuators. Moreover, SELFNET self-healing capabilities are not just about making remedies to faulty network components, they are also about providing safety, resilience and availability actively by providing not only reactive but also proactive measures. Therefore, SELFNET self-healing capabilities go beyond the traditional self-healing definition that follows a Break and Fix approach. If the network performance is downgrading or part of the infrastructure is failed in certain circumstances that may cause network failures and disruption of services, SELFNET self-healing capacities will also be triggered to take the most appropriate proactive healing actions based on SELFNET intelligence, which will allow the system to mitigate or avoid these failures and disruptions before they become critical. By extending the self-healing capabilities, the SELFNET framework can provide the network intelligence with self-detection, self-repairing, self-configuring and self-management features towards maximizing the reliability and availability of the 5G mobile network.

3.1 General background

Nowadays, networks are complex sets of heterogeneous and vendor-dependent equipment that use proprietary management applications. Consequently, when a network failure occurs or abnormal behaviours are detected, this complexity implies not only a huge cost but also a huge effort and a time-consuming process to manage the network elements, which prevents operators from improving network and service quality in a cost-effective manner. Therefore, it is expected that 5G infrastructure, integrated with new technologies such as SDN, NFV, SON and cloud computing, will lead to a major paradigm shift from configurable to programmable networks, which

will facilitate advanced self-healing capabilities. Firstly, the introduction of autonomic principles on SDN would enable an immediate detection and reparation of any malfunction or network failure [12]. Secondly, using NFV could significantly reduce the OPEX and service recreation/redeployment/recovery time. Therefore, SELFNET is expected to yield sustained quality of services under critical situations in terms of service continuity, availability and resilience by predicting/identifying network faults/failures and then making proactive/reactive remedies.

3.2 Self-healing relation to 5G visions

Enhanced physical and virtual infrastructure management and proactive detection and mitigation of network failures are crucial for realizing highly robust and usable 5G systems, especially for critical applications in addition to everyday operations. Self-healing use cases are expected to meet such requirements by means of intelligence-based self-monitoring, self-detection and self-organizing capabilities. In fact, through the deployment of SDN/NFV applications in the network infrastructure, SELFNET aids to achieve the automated network monitoring and maintenance of the network systems.

SELFNET self-healing concept follows the shift of 5G systems from reactive to proactive SON [13], by predicting the network failures by inferring network level intelligence from big context data and then take pre-emptive actions to resolve the problem before they occur. Moreover, SELFNET framework preserves the robustness and integrity of the 5G network, services provided via this network and the end-users' devices [14]. According to [15], “The future 5G infrastructure shall flexibly and rapidly adapt to a broad range of requirements”, which is the focus of the self-healing management capabilities. Moreover, in [14], “Preventing congestion and optimizing traffic management are essential on a mobile network and its importance will only grow with the industry moving towards 5G. High reliability and low latency will be key drivers for 5G services and can only be achieved with proper network management tools.” SELFNET self-healing measures provide self-detection, self-repairing and self-configuring features in the network infrastructure towards maximising the reliability, resilience, safety and availability of the 5G mobile network. Regarding performance and societal Key Performance Indicators (KPIs), SELFNET self-healing capabilities are in line with the following 5G-PPP KPIs [2, 15]:

Performance KPIs:

- “Increasing resilience, continuity, and much higher resource efficiency”
- “Creating a secure, reliable and dependable Internet with a “zero perceived” downtime for services provision”
- “Provide a reliable and trustworthy communications infrastructure, which secures critical infrastructures”
- “Reducing service creation reaching a complete deployment time from 90 h to 90 minutes”

Societal KPIs:

- Substantial reduction five in network management OPEX. 5G is expected to aid in ‘mission critical services requiring ultra-high reliability, global coverage and/or very low latency, which are up to now handled by specific networks, typically public safety, will become natively supported by the 5G infrastructure’.

4 Proactive self-healing for resource supply

Network infrastructures are constantly under pressure and test for their complex operations that demand sufficient resources supply. For instance, electricity supply is essential to keep the whole network system up and running for uninterrupted operations. Sensors can be deployed to monitor the energy distribution system, including generators and their power output, rack conditions, fluid leaks, batteries and temperature fluctuations in hot and cold aisles, in order to trigger alarms allowing proactive actions to be taken to correct problems/malfunctions before they become critical or lead to a serious outage. Moreover, an intelligent control of precision cooling and critical power may be performed in order to achieve better proactive self-healing capabilities. By extending and applying the concept in this power supply example to generic network resources, SELFNET self-healing targets to monitor not only physical but also virtual resources supply to ensure that the virtualized functions and operation environments will not fail due to the shortage or misallocation of the required resources, through the deployment of virtual resource broker actuators. This scenario is demonstrated in Figure 2.

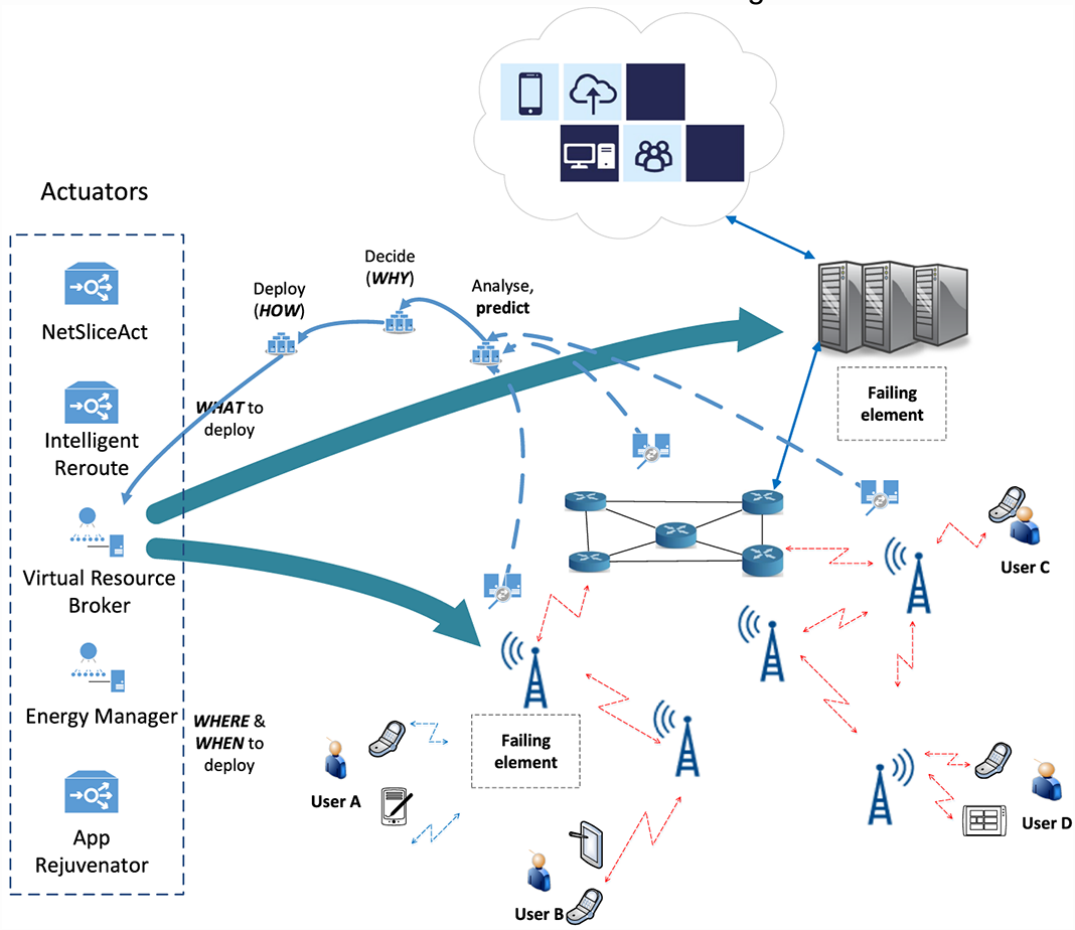

Figure 2. Proactive healing scenario.

To achieve the aforementioned scenario, firstly constant monitoring and control of the network resource usage and infrastructure performance will be in place to strengthen the robustness of the infrastructure. Furthermore, the self-healing analyzer will infer HoN metric reports based on infrastructure QoS metrics and SLA indicators. Consequently, the self-healing diagnosis intelligence will derive the potential problems, and the decision-making intelligence will release proactive healing responses. It should also be noted that all the information collected from the network infrastructure will be saved on a healing database, including the network response to the proactive healing actions. If the healing actions are unsuccessful, SELFNET must trigger a rollback mechanism returning the network infrastructure to a previous operational state. In another proactive self-healing scenario, an App running in the system may be ageing, which would lead to a crash if not dealt with in time. Once this is detected, an App rejuvenator actuator can be deployed to resolve this pending problem and thus avoid the potential crash.

5 Reactive Self-Healing in Critical and Unpredictable Scenarios

It is noted that not all the potential failures in the network can be predicted or identified in advance to allow proactive corrections. Therefore, SELFNET also offers reactive self-healing functionalities as a necessary backup, for example, a recovery action will be triggered when a failure is detected through the use of anomaly detection mechanisms in self-healing sensors, as illustrated in Figure 3. Moreover, if a critical failure occurs on the network infrastructure, for example, a network server or a link fails, SELFNET can deploy an intelligent reroute actuator in order to reroute the network traffic through alternative links, thereby reassuring reliability and availability to the current services operating on the network. The energy manager actuator in this case can also be used to switch off the failed network if it still consumes energy.

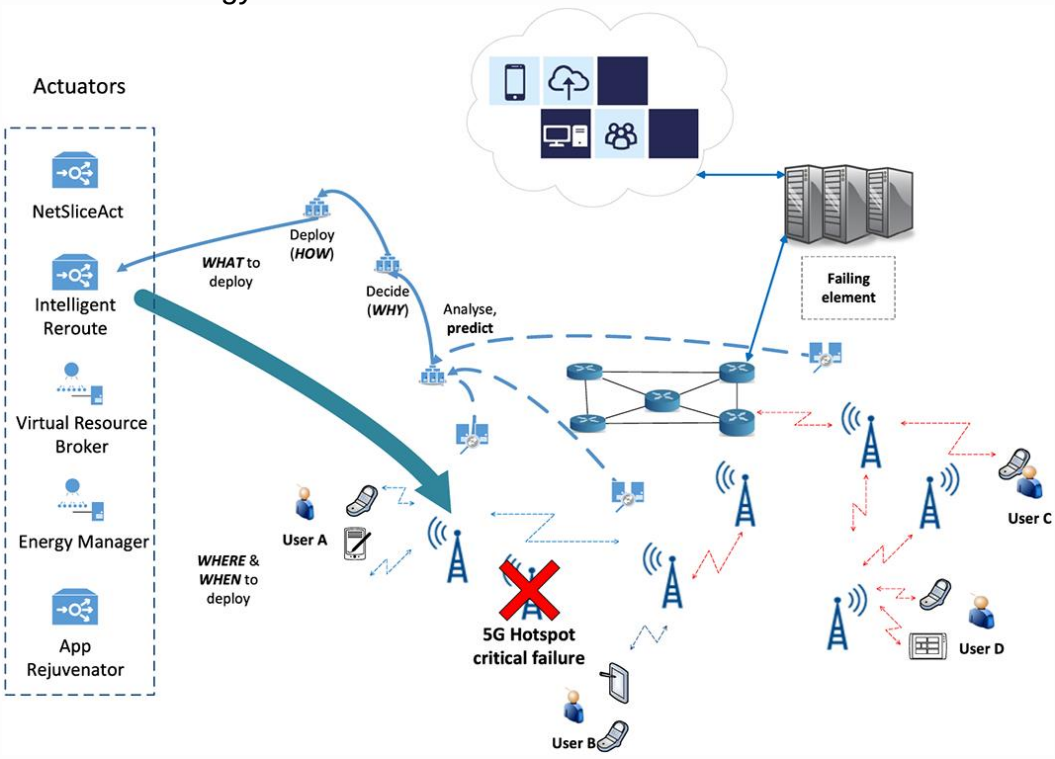

Figure 3. Reactive healing scenario.

In addition, prediction-based proactive actions may be unsuccessful, and as a result, a failure is not avoided. In this case, a fast reactive action is activated. Consequently, among other possible actions, an expedited deployment of a self-healing actuator may be determined and then executed in order to mitigate the failure/disruption and restore the system to normal operations. In case of an unpredictable software failure on a network element (e.g. a routing problem on a router) or a physical failure caused by a natural disaster, SELFNET self-healing aims to recover quickly, for example, by deploying speedy and cost-efficient recovery and redistribution mechanisms, in order to work around the failures, to recover at least partially first to minimize service disruption, for example, by providing an alternative network path to reroute the traffic. The main innovation in this reactive mode is the prompt and efficient service redeployment/recreation enabled by the SELFNET framework compared with existing recovery mechanisms in current network management systems.

6 Proactive Self-healing based on Network Slicing and Cyber-Footing Human Dynamics

It is commonly accepted that 5G will in particular address the needs of verticals, for example, new user groups with independent business models that depend on the availability of networking services. Examples are the automotive, automation, transport and logistics, intelligent traffic service, some e-health as well as public transportation industries. To describe the network services that the public networks have to provide in order to meet the specific needs of the verticals, the concept of network slices covering the connectivity and management functions is requested. In contrast to today's users of public network infrastructure, very strict requirements on safety, availability, coverage and security will have to be realized to make the implementation of the network slices unacceptably expensive. SELFNET self-healing concepts address this challenge by enabling a cost-efficient control of strict levels of coverage, redundancy and availability based on proactive measures as well as timely healing avoiding negative implications on the services of the verticals. Therefore, this use case scenario (Figure 4) demonstrates how SELFNET mechanisms can help to guarantee network slice functionalities in a cost-efficient way by providing actions re-establishing pre-defined levels of SLAs (resilience, security and availability) when they got lost through the deployment of NetSliceAct actuators.

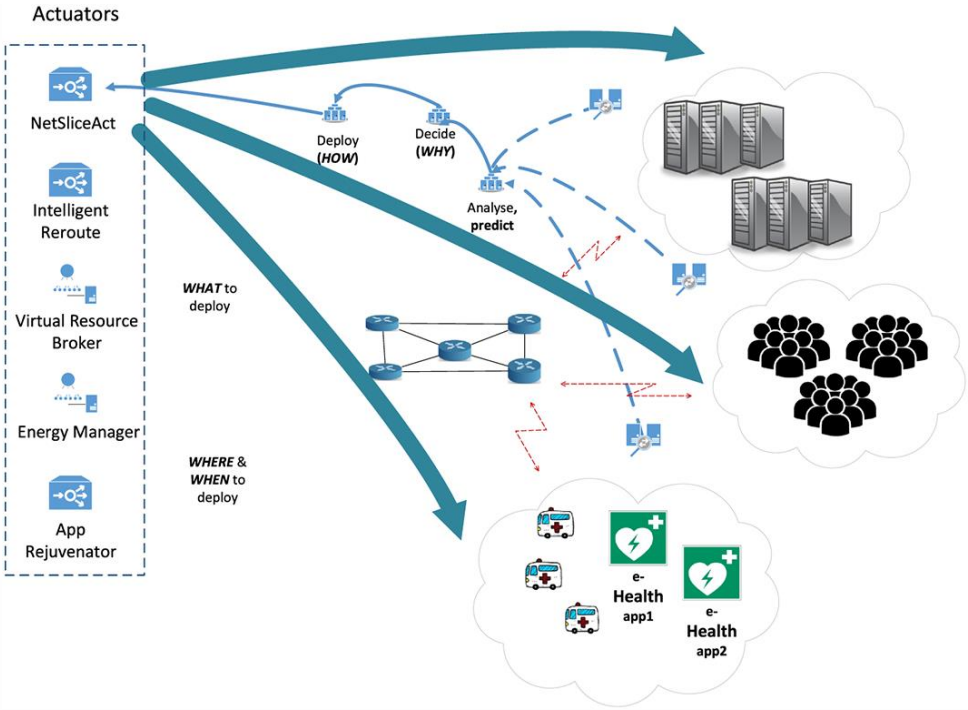

Figure 4. Network slicing scenario

To this end, SELFNET will collect historical references of the network elements and store them in a healing database. Based on this enhanced knowledge about the network performance and by using data mining and learning algorithms (identification of cyber-footing human dynamics and classification of infrastructure metrics), SELFNET can then predict high-resource demands before they happen and take actions before these demands lead to even more critical situations such as extreme mobile traffic bursts. The healing database also saves the unsuccessful responses, which means that these set of actions could not be taken in a similar situation. Thus, this enhanced knowledge will allow a better identification and classification of correlations between network behaviour and the users' social dynamics improving the proactive healing actions.

7 Self-Healing Contributions

The self-healing use case contributes with intelligent management capabilities to deal with a wide range of network malfunctions and failures in both reactive and proactive manners, which can not only remarkably reduce the OPEX of network operators but also improve the QoE/QoS of 5G systems. Therefore, this use case proposes self-healing mechanisms that will guarantee network slice functionalities based on strict levels of SLAs (resilience, redundancy and availability), taking advantage of proactive actions as well as fast-enough healing measures avoiding negative implications on the services of the verticals. For example, new user groups with independent business models and different QoS requirements will be serviced depending on the availability of networking services. In this way, SELFNET uses NetSliceAct actuators to establish, configure, monitor and re-establish a specific network slice profile within the physical infrastructure. Moreover, self-healing capabilities provide the identification of Cyber-Footing Human dynamics by using data mining and learning algorithms that will help to predict high-traffic demands

before they happen, which will allow an intelligent proactive response to alleviate the effect of these critical traffic mobile situations.

Moreover, the self-healing use case also introduce the use of infrastructure metrics and SLAs indicators for inferring HoN metric reports that will be used to detect existing or potential failures and malfunctions in the network infrastructure. Moreover, the use of context-aware information in the control plane and the detection of vulnerabilities on the virtual execution environment will enhance the self-healing capabilities of SELFNET. The deployment of reactive and proactive self-healing functionalities will automate the healing actions by means of self-organizing and self-configuring procedures to dynamically and flexibly deploy VNF actuators in the network infrastructure when and where needed.

Self-healing by addressing all these problems will imply the necessity of satisfy several conditions in order to accomplish all these contributions. One of the most basic requirements focuses on the problem of information management, such as collecting and storing data provided by the SELFNET actors or the ability of monitoring the pre-defined levels of SLAs previously mentioned. Reactions lead by the decision making planner are also taken into account. Because of this, SELFNET must be able to deploy sensors in order to monitor the network response to the self-healing actuators and access information on the healing database in order to enhance the self-healing recovery plan. In this way, SELFNET must also guarantee a fast deployment of multiple reactive/proactive recovery mechanisms and the ability to reverse them (rollback mechanism). On the other hand, SELFNET must be able also to detect vulnerabilities on the virtual execution environment, unexpected peaks on the network infrastructure and errors on the physical layer, such as link failures, hardware problems, energy output inconsistencies or misconfigurations. From these observations, SELFNET must have the potential of inferring infrastructure metrics, SLAs metrics, Cyber-Footing Human dynamics correlations, and with these, predict service disruptions or network failures before they occur. Regarding other general requirements, SELFNET in order to ensure its operation, the updating/modification of modules on repository must not affect the correct operation of sensors/actuators running on the infrastructure. Moreover, SELFNET must preserve isolated execution environment in accordance with the multi-tenancy capabilities.

8 Conclusions

In this paper, the proposed architecture of SELFNET has been briefly presented, which is divided into infrastructure layer, virtualized network layer, SON control layer, SON autonomic layer, SON interface layer and NFV orchestration and management. The novel management framework proposed by SELFNET takes advantage of new technologies such as SDN, NFV, artificial intelligence and cloud computing to provide self-healing, self-protection and self-optimization functionalities to the upcoming 5G mobile systems. Although SELFNET architecture is based on the combination of NFV and SDN standards proposed by ETSI and Open Networking Foundation, respectively, it goes far beyond. This paper also illustrated the self-healing use case, which can deal with the detected or predicted network failures in both reactive and preventive ways. The SLEFNET can not only reduce the OPEX of network operators but also can substantially improve QoE/QoS in terms of reliability, availability, service continuity and security.

Acknowledgements

This work is supported by the European Commission Horizon 2020 Programme under grant agreement number H2020-ICT-2014-2/671672 - SELFNET (Framework for Self-Organized Network Management in Virtualized and Software Defined Networks). Ángel Leonardo Valdivieso Caraguay and Lorena Isabel Barona López are supported by the Secretaría Nacional de Educación Superior, Ciencia, Tecnología e Innovación SENESCYT (Quito, Ecuador).

References

[1] 1ETSI Industry Specification Group (ISG). Network Function Virtualization (NFV) Use Cases, October 2013. Available from: http://www.etsi.org/deliver/etsi_gs/nfv/001_099/001/01.01.01_60/gs_nfv001v010101p.pdf/ [Accessed on September 2015].

[2] 25GPP. Advanced 5G Network Infrastructure for the Future Internet. Available from: https://5g-ppp.eu/wp-content/uploads/2014/02/Advanced-5G-Network-Infrastructure-PPP-in-H2020_Final_November-2013.pdf/ [Accessed on September 2015].

[3] 3Kobayashi M, Seetharaman S, Parulkar G, Appenzeller G, Little J, Reijendam V, et al.. Maturing of openflow and software-defined networking through deployments. *Computer Networks* 2014; 61: 151–175.

[4] 4Feamster N, Rexford J, Zegura E. The road to SDN: an intellectual history of programmable networks. *ACM SIGCOMM Computer Communication Review* 2014; 44: 87–98.

[5] 5Sanchez J, Yahia B, Grida I, Crespi N, Rasheed T, Siracusa D. Softwarized 5G Networks Resiliency with self-healing. In *1st International Conference on 5G for Ubiquitous Connectivity (5GU)*, Akaslompolo, 2014; 229–233.

[6] 6ETSI Industry Specification Group (ISG). Network function virtualization (NFV) architectural framework, October 2013. Available from: http://www.etsi.org/deliver/etsi_gs/nfv/001_099/002/01.01.01_60/gs_nfv002v010101p.pdf/ [Accessed on September 2015].

[7] 7Mijumbi R, Serrat J, Gorricho JL, Bouten N, De Turck F, Boutaba R. Network function virtualization: state-of-the-art and research challenges. *Communications Surveys Tutorials IEEE* 2015; 99: 1–28.

[8] 8Barona López LI, Valdivieso Caraguay AL, García Villalba LJ, López D. Trends on virtualisation with software defined networking and network function virtualisation. *IET Networks* 2015; 4: 255–263.

[9] 9Open Networking Foundation (ONF). OpenFlow-enabled SDN and network function virtualization, February 2014. Available from: https://www.opennetworking.org/images/stories/downloads/sdn-resources/solution-briefs/sb-sdn-nvf-solution.pdf/ [Accessed on September 2015].

[10] 10ETSI Industry Specification Group (ISG). Network function virtualisation. Available from: http://www.etsi.org/technologies-clusters/technologies/nfv/ [Accessed on November 2015].

[11] 11Armbrust M, Fox A, Griffith R, et al.. A view of cloud computing. *Communications of the ACM* 2010; 53: 50–58.

[12] 12Vilchez JMS, Yahia IGB, Crespi N. Self-healing mechanisms for software defined networks. In *8th International Conference on Autonomous*

Infrastructure, Management and Security (AIMS): Brrno, Czech Republic, 2014.

[13] 13Imran A, Zoha A. Challenges in 5G: how to empower SON with big data for enabling 5G. *Network IEEE* 2014; 28: 27–33.

[14] 145G-PPP. Specialized services, network management and 5G, May 2015. Available from: https://5g-ppp.eu/wp-content/uploads/2015/06/Specialized-Services-Network-Management-and-5G.pdf/ [Accessed on September 2015].

[15] 155G Vision. The 5G Infrastructure Public Private Partnership, February 2015. Available from: https://5g-ppp.eu/wp-content/uploads/2015/02/5G-Vision-Brochure-v1.pdf/ [Accessed on September 2015].